

CLAIMS

What is claimed is

- 1 1. A method of securely invoking an access control function, the method comprising
2 the steps of:
3 receiving a digital signature for the access control function;
4 generating a mapping of the access control function to the digital signature;
5 determining that the digital signature is mapped to the access control function
6 based on the mapping when execution of the access control function is
7 requested;
8 determining whether an executable element matches the access control function
9 based on the digital signature; and
10 executing the executable element only when the executable element matches the
11 access control function.
- 1 2. The method of Claim 1,
2 wherein a particular class defines an implementation for the access control
3 function;
4 wherein the step of receiving a digital signature includes the step of receiving a
5 digital signature for the particular class; and
6 wherein the step of generating a mapping includes generating a mapping between
7 the particular class and the digital signature.
- 1 3. The method of Claim 1,
2 wherein the method further includes the step of detecting that an access control
3 event has occurred; and
4 wherein the step of retrieving the executable element is performed in response to
5 detecting that the event has occurred.

- 1 4. The method of Claim 3,
2 wherein the method further includes the steps of:
3 generating a mapping between the access control event and the access
4 control function;
5 determining that the access control event is mapped to the access control
6 function; and
7 wherein the step of retrieving the executable element is performed in response to
8 determining that the access control event is mapped to the access control
9 function.
- 1 5. The method of Claim 4, further including the step of the executable element
2 returning name-value pairs.
- 1 6. The method of Claim 5, wherein the step of the executable element returning
2 name-value pairs includes the executable element returning a hash table that
3 contains the name-value pairs.
- 1 7. The method of Claim 1, wherein the method further includes the steps of:
2 generating a mapping of a plurality of access control functions to digital
3 signatures, wherein the plurality of access control functions include the
4 access control function, wherein one or more classes define an
5 implementation for each of the plurality of access control functions; and
6 wherein each of the one or more classes belong to a superclass.
- 1 8. The method of Claim 7, further including the step of invoking a routine defined
2 by a superclass that collects data to return to a caller of the particular class.
- 1 9. The method of Claim 8, wherein the step of executing the executable element
2 includes invoking a routine defined for the superclass.

- 1 10. The method of Claim 1, wherein the step of retrieving an executable element
2 includes retrieving byte code.
- 1 11. The method of Claim 10, wherein the step of retrieving byte code includes
2 retrieving Java byte code.
- 1 12. The method of Claim 1, wherein the step of retrieving an executable element
2 includes a first computer system retrieving byte code transmitted via a local area
3 network from a second computer system.
- 1 13. A computer-readable medium carrying one or more sequences of one or more
2 instructions for securely invoking an access control function, the one or more
3 sequences of one or more instructions including instructions which, when
4 executed by one or more processors, cause the one or more processors to perform
5 the steps of:
6 receiving a digital signature for the access control function;
7 generating a mapping of the access control function to the digital signature;
8 determining that the digital signature is mapped to the access control function
9 based on the mapping when execution of the access control function is
10 requested;
11 determining whether an executable element matches the access control function
12 based on the digital signature; and
13 executing the executable element only when the executable element matches the
14 access control function.
- 1 14. The computer-readable medium of Claim 13,
2 wherein a particular class defines an implementation for the access control
3 function;

4 wherein the step of receiving a digital signature includes the step of receiving a
5 digital signature for the particular class; and
6 wherein the step of generating a mapping includes generating a mapping between
7 the particular class and the digital signature.

1 15. The computer-readable medium of Claim 13,
2 wherein the computer-readable medium further includes sequences of instructions
3 for performing the step of detecting that an access control event has
4 occurred; and
5 wherein the step of retrieving the executable element is performed in response to
6 detecting that the event has occurred.

1 16. The computer-readable medium of Claim 15,
2 wherein the computer-readable medium further includes sequences of instructions
3 for performing the steps of:
4 generating a mapping between the access control event and the access
5 control function;
6 determining that the access control event is mapped to the access control
7 function; and
8 wherein the step of retrieving the executable element is performed in response to
9 determining that the access control event is mapped to the access control
10 function.

1 17. The computer-readable medium of Claim 16, further including sequences of
2 instructions for performing the step of the executable element returning name-
3 value pairs.

- 1 18. The computer-readable medium of Claim 17, wherein the step of the executable
2 element returning name-value pairs includes the executable element returning a
3 hash table that contains the name-value pairs.
- 1 19. The computer-readable medium of Claim 13, wherein the computer-readable
2 medium further includes sequences of instructions for performing the steps of:
3 generating a mapping of a plurality of access control functions to digital
4 signatures, wherein the plurality of access control functions include the
5 access control function, wherein one or more classes define an
6 implementation for each of the plurality of access control functions; and
7 wherein each of the one or more classes belong to a superclass.
- 1 20. The computer-readable medium of Claim 19, further including sequences of
2 instructions for performing the step of invoking a routine defined by a superclass
3 that collects data to return to a caller of the particular class.
- 1 21. The computer-readable medium of Claim 20, wherein the step of executing the
2 executable element includes invoking a routine defined for the superclass.
- 1 22. The computer-readable medium of Claim 13, wherein the step of retrieving an
2 executable element includes retrieving byte code.
- 1 23. The computer-readable medium of Claim 22, wherein the step of retrieving byte
2 code includes retrieving Java byte code.
- 1 24. The computer-readable medium of Claim 13, wherein the step of retrieving an
2 executable element includes a first computer system retrieving byte code
3 transmitted via a local area network from a second computer system.

- 1 25. An access control system, comprising:
2 a processor;
3 a memory coupled to the processor;
4 a first mapping that maps each of a set of access control functions to a digital
5 signature of that access control function;
6 the processor configured to retrieve an executable element in response to a
7 request to execute a first access control function;
8 the processor configured to determine whether the executable element matches the
9 first access control function based on the digital signature; and
10 the processor configured to execute the executable element when the executable
11 element matches the first access control function.
- 1 26. The access control system of Claim 25,
2 wherein the set of access control functions are each implemented in a class; and
3 wherein the first mapping maps a class implementing one of the set of access
4 control functions to a digital signature.
- 1 27. The access control system of Claim 25, further comprising:
2 the processor configured to detect that an access control event has occurred; and
3 the processor configured to retrieve the executable element in response to
4 detecting that the event has occurred.
- 1 28. The access control system of Claim 27, further comprising:
2 the processor configured to generate a mapping between the access control event
3 and the access control function;
4 the processor configured to determine that the access control event is mapped to
5 the access control function; and

6 the processor configured to retrieve the executable element in response to
7 determining that the access control event is mapped to the access control
8 function.

1 29. The access control system of Claim 28, wherein the executable element returns
2 name-value pairs.

1 30. The access control system of Claim 29, wherein the executable element returns a
2 hash table that contains the name-value pairs.

1 31. The access control system of Claim 25,
2 wherein the processor is configured to generate a mapping of a plurality of access
3 control functions to digital signatures;
4 wherein the plurality of access control functions include the access control
5 function, wherein one or more classes define an implementation for each
6 of the plurality of access control functions; and
7 wherein each of the one or more classes belong to a superclass.

1 32. The access control system of Claim 31, further comprising said processor
2 configured to invoke a routine defined by a superclass that collects data to return
3 to a caller of the particular class.

1 33. The access control system of Claim 32, wherein said processor is configured to
2 execute the executable element by invoking a routine defined for the superclass.

1 34. The access control system of Claim 33, wherein said executable element is byte
2 code.

1 35. The access control system of Claim 34, wherein said byte code includes Java byte
2 code.

- 1 36. The access-control system of Claim 35, wherein said processor is configure to
2 retrieve an executable element by retrieving byte code transmitted via a local area
3 network.

SECRET